

PATENT ABSTRACTS OF JAPAN

(11)Publication number : 2001-147984

(43)Date of publication of application : 29.05.2001

(51)Int.Cl.

G06F 19/00
G09C 1/00

(21)Application number : 11-331274

(71)Applicant : NTT DATA CORP

(22)Date of filing : 22.11.1999

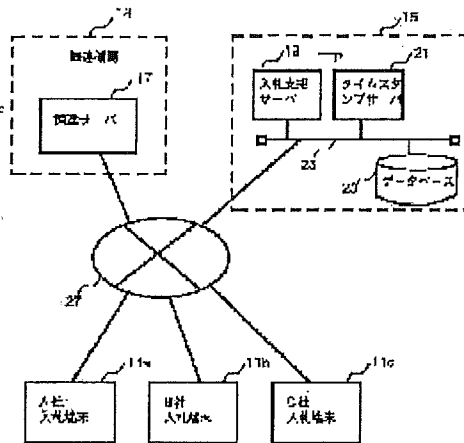
(72)Inventor : MOTONAGA KIMIAKI

(54) SYSTEM AND METHOD FOR ELECTRONIC VOTING

(57)Abstract:

PROBLEM TO BE SOLVED: To enable high-reliability electronic tendering, with which illegality can be surely verified.

SOLUTION: Each of tendering terminals 11a, 11b and 11c generates the hash value of a tender document, enciphers the document with its own secret key and transmits the enciphered hash document to a TTP 15. The TTP prepares an SHV certificate concerning each of enciphered hash documents and calculates an SHV every second. The TTP discloses the SHV of every second of each of enciphered hash documents and each of enciphered hash documents, to which the SHV certificate is attached, on the Internet 27. Before tendering to a procurement institution 13, each of tendering terminals downloads the enciphered hash document with SHV certificate. The procurement institution discloses a tender document 107 of a successful bidder company. Each of tendering terminal downloads the tender document of the successful bidder company, takes the hash thereof, deciphers the hash value after successful bid and the enciphered hash document of the successful bidder company, compares the deciphered value with the hash value before the successful bid and when these values are not coincident, it is judged the tender document of the successful bid is illegally revised.



(19) 日本国特許庁 (J P)

(12) 公開特許公報 (A)

(11) 特許出願公開番号

特開2001-147984

(P2001-147984A)

(43) 公開日 平成13年5月29日(2001.5.29)

(51) Int.Cl. ⁷	識別記号	F I	テーマコード*(参考)
G 0 6 F 19/00		G 0 9 C 1/00	6 4 0 Z 5 B 0 4 9
G 0 9 C 1/00	6 4 0	G 0 6 F 15/28	B 5 J 1 0 4
			9 A 0 0 1

審査請求 有 請求項の数23 O L (全 14 頁)

(21) 出願番号 特願平11-331274

(22) 出願日 平成11年11月22日(1999. 11. 22)

(71) 出願人 000102728

株式会社エヌ・ティ・ティ・データ

東京都江東区豊洲三丁目3番3号

(72) 発明者 本永 公章

東京都江東区豊洲三丁目3番3号 株式会社
エヌ・ティ・ティ・データ内

(74) 代理人 100095371

弁理士 上村 輝之

Fターム(参考) 5B049 AA05 BB36 CC01 CC31 EE03

EE05 GG04 GG07 GG10

5J104 AA08 LA03 LA05 MA02 NA12

PA07 PA17

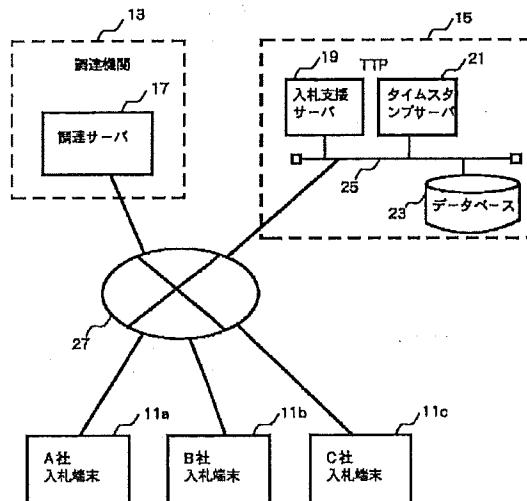
9A001 EE03 JJ25 JJ27 JJ71 LL03

(54) 【発明の名称】 電子投票方式、及び方法

(57) 【要約】 (修正有)

【課題】 不正を確実に検証できる信頼性高い電子入札。

【解決手段】 各入札端末11a、11b、11cは、入札文書のハッシュ値を生成してそれを自分の秘密鍵で暗号化し、その暗号化ハッシュ文書をTTP15に送信する。TTPは、各暗号化ハッシュ文書について、SHV証明書を作成し、且つ、毎秒SHVを算出する。TTPは、各暗号化ハッシュ文書の毎秒のSHVと、SHV証明書を添付した各暗号化ハッシュ文書を、インターネット27上に公開する。各入札端末は、調達機関13に入札する前に、SHV証明書付きの暗号化ハッシュ文書をダウンロードしておく。調達機関は、落札社の入札文書107を公開する。各入札端末は、落札社の入札文書をダウンロードして、そのハッシュ値と、開札後のハッシュ値と、落札社の暗号化ハッシュ文書を復号化して開札前のハッシュ値とを比較し、それらが一致していなければ、落札された入札文書は不正に改竄されたと判断する。



【特許請求の範囲】

【請求項1】 投票書類の内容を記録した投票書類データを生成する1又は複数の情報処理装置と、信頼される第三者機関と、前記投票書類データが調達される機関とを備え、

前記第三者機関が、暗号化された前記投票書類データの各々を公開するための手段を備え、

前記調達機関が、前記調達された投票書類データの各々に基づき開票の結果を示すデータを公開するための手段を備え、

前記1又は複数の情報処理装置が、

前記投票書類データを暗号化してそれを前記第三者機関に送るための第1の送り手段と、

前記投票書類データを前記調達機関に送るための第2の送り手段と、

前記公開された暗号化投票書類データを入手するための第1の入手手段と、

前記公開された開票結果データを入手するための第2の入手手段と、

不正の有無を検知するために、前記開票結果データと前記暗号化投票書類データとを比較する手段とを備える電子投票方式。

【請求項2】 前記第三者機関において、

前記暗号化投票書類データの各々に対し、日時を付けてその投票書類データの存在を証明する証明書を生成する手段が更に備えられ、

前記公開するための手段が、前記生成した証明書の各々を、それらに対応する前記暗号化投票書類データに添付して公開するようにし、

前記1又は複数の情報処理装置において、

前記第1の入手手段が、前記公開された前記暗号化投票書類データと共に前記証明書を入手し、

前記比較する手段が、不正の有無を検知するために、前記開票の日時と、前記入手した証明書に付けられた日時とを更に比較する請求項1記載の電子投票方式。

【請求項3】 前記1又は複数の情報処理装置において、

前記投票書類データの特徴データを生成する手段が更に備えられ、

前記第1の送り手段が、前記特徴データを暗号化したものを前記第三者機関に送るようにし、

前記第三者機関において、

前記公開するための手段が、前記暗号化特徴データの各々を公開するようにし、

前記1又は複数の情報処理装置において、

前記第1の入手手段が、前記公開された暗号化特徴データを入手し、

前記比較する手段が、不正の有無を検知するために、前記開票結果データの特徴データを生成し、その開票結果データの特徴データと、前記入手した暗号化特徴データ

とを比較する請求項1記載の電子投票方式。

【請求項4】 前記第三者機関において、

前記証明書に付けられた日時以後、任意の時に前記暗号化特徴データの別特徴データを生成する手段と、

前記任意の時に生成した別特徴データを公開するための手段が更に備えられ、

前記証明書を生成する手段が、前記暗号化特徴データの各々に対し、前記暗号化特徴データの別特徴データを生成した日時と、その日時に生成した別特徴データを前記

10 暗号化特徴データを用いて生成するための方法とを記録した証明書を生成し、

前記1又は複数の情報処理装置において、

前記比較する手段が、不正の有無を検知するために、前記公開された別特徴データから、前記比較の対象の特徴データに対応する証明書に記録された生成日時の際の別特徴データを入手し、且つ、前記比較対象の特徴データとその証明書に記録された前記生成方法とに基づいて前記比較対象の特徴データの別特徴データを生成し、その生成した別特徴データと前記入手した別特徴データとを比較する請求項2又は3記載の電子投票方式。

【請求項5】 前記特徴データ又は前記別特徴データは、ハッシュ値である請求項3又は4記載の電子投票方式。

【請求項6】 前記1又は複数の情報処理装置において、前記第2の送り手段が、前記入手した証明書のうち、前記生成した投票書類データに対応する証明書をその投票書類データに添付して、それを前記調達機関に送るようにする請求項2乃至請求項5のいずれか一項記載の電子投票方式。

30 【請求項7】 前記開票の後に、前記投票の参加者から不正があった旨が報知されたときは、

前記1又は複数の情報処理装置において、

前記第1又は第2の入手手段が、前記報知を行なった投票参加者が保持する投票書類データを入手するようにし、

前記比較する手段が、前記報知の内容が真実か否かを検知するために、前記報知を行なった投票参加者の投票書類データと、前記入手した暗号化投票書類データ又は暗号化特徴データのうち前記報知した投票参加者のものに該当するデータとを比較する請求項1乃至請求項6のうちのいずれか一項記載の電子投票方式。

【請求項8】 前記1又は複数の情報処理装置において、前記第2の送り手段が、前記投票書類データ又はその特徴データを暗号化して前記調達機関に送るようにする請求項1乃至請求項7のうちのいずれか一項記載の電子投票方式。

【請求項9】 前記第三者機関において、前記公開するための手段が、コンピュータネットワーク上に前記暗号化投票書類データ又は前記暗号化特徴データの各々を公開する請求項1乃至請求項8のうちのいずれか一項記載

の電子投票方式。

【請求項10】 前記調達機関において、前記公開するための手段が、コンピュータネットワーク上に前記開票結果データを公開する請求項1乃至請求項9のうちのいずれか一項記載の電子投票方式。

【請求項11】 前記暗号化投票書類データ又は前記暗号化特徴データは、前記第三者機関の公開鍵で暗号化されており、前記第三者機関が、前記開票のときに前記第三者機関の秘密鍵を発行する請求項1乃至請求項10のうちのいずれか一項記載の電子投票方式。

【請求項12】 前記1又は複数の情報処理装置において、

前記第1の送り手段が、前記投票書類データ又はその特徴データを自分の秘密鍵又は共通鍵で暗号化して前記第三者機関に送り、

前記第2の送り手段が、前記秘密鍵又は共通鍵で暗号化された投票書類データ又はその特徴データを前記第三者機関の公開鍵で更に暗号化して前記調達機関に送り、前記調達機関において、

前記開票のときに前記第三者機関の秘密鍵を受けて、その秘密鍵で、前記公開鍵で更に暗号化された前記暗号化投票書類データ又は前記暗号化特徴データの各々を復号化する手段と、

その復号化した前記暗号化投票書類データ又は前記暗号化特徴データの各々を、それらに対応する前記1又は複数の情報処理装置の公開鍵又は共通鍵で復号化する手段とが更に備えられる請求項1乃至請求項11のうちのいずれか一項記載の電子投票方式。

【請求項13】 前記1又は複数の情報処理装置と、前記第三者機関と、前記調達機関とがコンピュータネットワークを介して通信可能に接続されており、

前記1又は複数の情報処理装置において、

前記第1の送り手段が、前記投票書類データ又はその特徴データを暗号化してそれを前記コンピュータネットワークを介して前記第三者機関に送信し、

前記第2の送り手段が、前記投票書類データ、その特徴データ、前記暗号化投票書類データ、又は前記暗号化特徴データを暗号化してそれを前記コンピュータネットワークを介して前記調達機関に送信する請求項1乃至請求項12のうちのいずれか一項記載の電子投票方式。

【請求項14】 前記開票結果データには、前記開票の際に選出された投票書類データが含まれており、

前記1又は複数の情報処理装置において、前記比較する手段が、前記選出された投票書類データと、前記入手した暗号化投票書類データ又は暗号化特徴データのうち前記選出された投票書類データに対応するデータとを比較する請求項1乃至請求項13のうちのいずれか一項記載の電子投票方式。

【請求項15】 前記投票書類データは、入札のときの提出書類の内容を示すデータである請求項1乃至請求項

14のうちのいずれか一項記載の電子投票方式。

【請求項16】 投票書類の内容を記録した投票書類データが暗号化されたものの各々を公開するためのステップと、

前記投票書類データが調達される機関において調達された投票書類データの各々に基づく開票の結果を示すデータを公開するためのステップと、

不正の有無を検知するために、前記公開された暗号化投票書類データと前記公開された開票結果データとを比較するステップとを有する電子投票方法。

【請求項17】 前記暗号化投票書類データの各々に対し、日時を付けてその投票書類データの存在を証明する証明書を生成するステップを更に有し、

前記公開するためのステップが、前記生成した証明書の各々を、それらに対応する前記暗号化投票書類データに添付して公開するようにし、

前記比較するステップが、不正の有無を検知するために、前記公開された前記暗号化投票書類データに添付された前記証明書に付けられた日時と、前記開票の日時とを更に比較する請求項16記載の電子投票方法。

【請求項18】 投票書類の内容を記録した投票書類データを生成する手段と、

前記投票書類データを暗号化する手段と、

複数の投票参加者の暗号化された投票書類データの各々が公開されたものから暗号化投票書類データを入手するための第1の入手手段と、

投票書類データの各々が調達されたことに基づく開票の結果を示す、公開されたデータを入手するための第2の入手手段と、

不正の有無を検知するために、前記入手した開票結果データと前記暗号化投票書類データとを比較する手段とを備える情報処理装置。

【請求項19】 第1の入手手段が、投票書類データの存在を証明する証明書が添付された、暗号化書類データを入手し、

前記比較する手段が、不正の有無を検知するために、前記開票の日時と、前記入手した証明書に付けられた日時とを更に比較する請求項18記載の情報処理装置。

【請求項20】 前記投票書類データの特徴データを生成する手段を更に備え、

前記暗号化する手段が、前記特徴データを暗号化し、

前記第1の入手手段が、複数の投票参加者の暗号化された特徴データの各々が公開されたものから暗号化特徴データを入手するための、

前記比較する手段が、不正の有無を検知するために、前記開票結果データの特徴データを生成し、その開票結果データの特徴データと、前記入手した暗号化特徴データとを比較する請求項18記載の情報処理装置。

【請求項21】 前記証明書には、前記暗号化特徴データの別特徴データが生成された日時と、その日時に生成

10

20

30

40

50

した別特徴データを前記暗号化特徴データを用いて生成するための方法とが記録されており、前記比較する手段が、不正の有無を検知するために、前記存在した日時以後に任意の時に生成された別特徴データが公開されたものから、前記比較の対象の特徴データに対応する証明書に記録された生成日時の際の別特徴データを入手し、且つ、前記比較対象の特徴データとそれの証明書に記録された前記生成方法とに基づいて前記比較対象の特徴データの別特徴データを生成し、その生成した別特徴データと前記入手した別特徴データとを比較する請求項19又は20記載の情報処理装置。

【請求項22】 前記開票の後に、前記投票の参加者から投票書類データの各々が調達された機関において不正があった旨が報知されたときは、前記第1又は第2の入手手段が、前記報知を行なった投票参加者が保持する投票書類データを入手するようにし、前記比較する手段が、前記報知の内容が真実か否かを検知するために、前記報知を行なった投票参加者の投票書類データと、前記入手した暗号化投票書類データ又は暗号化特徴データのうち前記報知した投票参加者のものに該当するデータとを比較する請求項18乃至請求項21のうちのいずれか一項記載の情報処理装置。

【請求項23】 信頼される第三者機関と、投票書類の内容を記録した投票書類データを生成する1又は複数の情報処理装置と、前記投票書類データが調達される機関とが備えられるシステム上で、前記情報処理装置としてコンピュータを機能させるためのプログラムを記録したコンピュータ読取可能な記録媒体において、投票書類の内容を記録した投票書類データを生成する手段と、前記投票書類データを暗号化する手段と、複数の投票参加者の暗号化された投票書類データの各々が公開されたものから暗号化投票書類データを入手するための第1の入手手段と、投票書類データが調達されたことに基づく開票の結果を示す、公開されたデータを入手するための第2の入手手段と、不正の有無を検知するために、前記公開された開票結果データと前記公開された暗号化投票書類データとを比較する手段とを前記コンピュータに実行させるためのプログラムコードを含んだコンピュータ読取可能な記録媒体。

【発明の詳細な説明】

【0001】

【発明の技術分野】本発明は、コンピュータを利用した電子投票の方式に関する。

【0002】

【従来の技術】コンピュータを利用した電子投票の代表的なものとして、電子入札が知られているが、電子入札

の方式としては、TTP(Trusted Third Party、信頼される第三者機関(第三者認証機関))を用いた時間鍵方式が知られている。この方式では、TTP、入札参加者、及び調達機関との間で、一般に、図1、2に示すような動作が行なわれている。

【0003】まず、図1に示すように、TTP5が、公開鍵と秘密鍵のペアを作成して(ステップS1)、公開鍵のみを調達機関3に送信する(S2)。その後、調達機関3は、入札参加者1a、1b、1cから入札参加申請を受けたら(S3、4、5)、それに対して、TTP5から受けた公開鍵をその入札参加者1a、1b、1cに配布する(S6、7、8)。

【0004】各入札参加者1a、1b、1cは、調達機関3から公開鍵を受取った後、図2に示すように、その公開鍵を使用して入札のための提出書類(以下、入札文書)を暗号化し(ステップS9、10、11)、それを調達機関3に送信することで入札する(S12、13、14)。TTP5は、開札時刻になったときに、秘密鍵を調達機関3に送信する(S15)。調達機関3は、TTP5からの秘密鍵を使用して公開鍵で暗号化されている入札文書を復号化し、開札を行なう(S16)。

【0005】

【発明が解決しようとする課題】入札では、不正の防止が何よりも望まれることである。しかし、上述した電子入札は、以下のような不正が行われても、これを電子的に発見し防止することができない。

【0006】(1) 調達機関3が、受け付けた入札文書を開札後に改竄することこれにより、調達機関3が、ある入札参加者1aと不正に契約を結んで、その参加者1aが落札できるような入札文書に改竄することが可能になってしまう。

【0007】(2) 調達機関3が、提出期限を過ぎていても拘わらず入札文書を受け付けることこれにより、ある入札参加者1aが、何らかの方法で他の入札参加者1b、1cの動向を探り、他の入札参加者1b、1cが入札文書を調達機関3に提出した後に、それに応じて、自分に都合の良い文書を作成して入札することが可能になってしまう。

【0008】(3) 入札参加者1a、1b、1cが、入札又は開札後に、自分の手元にある入札文書の内容を不正に改竄することこれにより、入札参加者1a、1b、1cは、落札できなかった場合に、「現在、調達機関3に存在している入札文書は、調達機関3で不正に改竄されたものであり、自分が入札したものとは異なる」と主張することが可能になってしまう。

【0009】従って、本発明の目的は、上記不正を確実に検証できる信頼性の高い電子入札を提供することにある。

【0010】

【課題を解決するための手段】本発明の第1の側面に従

う電子投票方式では、投票書類の内容を記録した投票書類データを生成する1又は複数の情報処理装置と、信頼される第三者機関と、前記投票書類データが調達される機関とを備え、第三者機関が、暗号化された投票書類データを公開するための手段を備え、調達機関が、調達された投票書類データに基づく投票結果を示すデータを公開するための手段を備え、1又は複数の情報処理装置が、投票書類データを暗号化してそれを第三者機関に送るための手段と、投票書類データを調達機関に送るための手段と、公開された暗号化投票書類データを入手するための手段と、公開された投票結果データを入手するための手段と、不正の有無を検知するために、暗号化投票書類データと投票結果データとを比較する手段とを備える。

【0011】例えば、1又は複数の情報処理装置は、投票書類データを信頼される第三者機関に送るときは、第三者機関の公開鍵や自分の共通鍵又は秘密鍵で暗号化した投票書類データを、フロッピーディスクやMO等の記録媒体に記録してその記録媒体を郵送などで送るようにしたり、コンピュータネットワーク（典型的にはインターネット）を介して送信したりする。また、1又は複数の情報処理装置は、投票書類データを調達機関に送るときは、投票書類データを、フロッピーディスク等の記録媒体に記録してその記録媒体を郵送などで送るようにしたり、第三者機関の公開鍵で暗号化、或いは自分の共通鍵又は秘密鍵で暗号化（更に第三者機関の公開鍵で暗号化してもよい）してからそれをコンピュータネットワークを介して送信したりする。第三者機関は、送られて来た各記録媒体に記録された、又はコンピュータネットワークを介して送られて来た暗号化投票書類データを、コンピュータネットワーク上に、特定の雑誌上に、又はCD-ROMやMO等の記録媒体に記録して各入札参加社宛に郵送等で送って直接的に、のいずれかの方法で公開するようにする。調達機関は、郵送等で送られて来た各記録媒体に記録された、又はコンピュータネットワークを介して送られて来た投票書類データの各々に基づく開票の結果を示すデータ（例えば、調達機関で調達された投票書類データの全て、又は開票において選出された投票書類データのみ）を、コンピュータネットワーク上に、特定の雑誌上に、又はCD-ROMやMO等の記録媒体に記録して各入札参加社宛に郵送等で送って直接的に、のいずれかの方法で公開するようにする。1又は複数の情報処理装置は、第三者機関、及び調達機関によって行なわれる上記公開により、開票結果データと、投票参加者の暗号化投票書類データとを入手し、不正の有無を検知するために、開票結果データと暗号化投票書類データとを比較する。比較するときは、例えば、各投票参加者の共通鍵又は公開鍵で、暗号化投票書類データの各々を復号化してから、上記比較をする。この結果、実質的に一致しないデータが含まれていれば、投票書類データ

タが不正に改竄されたということを検知することができる。

【0012】好適な実施形態では、第三者機関において、暗号化投票書類データの各々に対し、日時を付けてその投票書類データの存在を証明する証明書を生成する手段が更に備えられ、公開するための手段が、生成した証明書の各々を、それらに対応する暗号化投票書類データに添付して公開するようにする。この場合、1又は複数の情報処理装置において、第1の入手手段が、公開された暗号化投票書類データと共に証明書を入手し、比較する手段が、不正の有無を検知するために、開票の日時と、入手した証明書に付けられた日時とを更に比較する。これにより、証明書に付けられた日時が開票日時よりも遅い日時であるものが含まれていれば、開票日時が過ぎたにも拘わらずに不正に受け付けられた投票書類データがあることを検知することができる。

【0013】好適な実施形態では、1又は複数の情報処理装置において、投票書類データの特徴データを生成する手段が更に備えられ、第1の送り手段が、特徴データを暗号化したものを第三者機関に送るようにする。第三者機関において、公開するための手段が、暗号化特徴データの各々を公開するようにする。この場合、1又は複数の情報処理装置において、第1の入手手段が、公開された暗号化特徴データを入手し、比較する手段が、不正の有無を検知するために、開票結果データの特徴データを生成し、その開票結果データの特徴データと、入手した暗号化特徴データとを比較する。

【0014】好適な実施形態では、第三者機関において、上記証明書に付けられた日時以後、任意の時に暗号化特徴データの別特徴データを生成する手段と、その任意の時に生成した別特徴データを公開するための手段が更に備えられ、証明書を生成する手段が、暗号化特徴データの各々に対し、暗号化特徴データの別特徴データを生成した日時と、その日時に生成した別特徴データをその暗号化特徴データを用いて生成するための方法とを記録した証明書（例えばSHV証明書）を生成する。この場合、1又は複数の情報処理装置において、比較する手段が、不正の有無を検知するために、公開された別特徴データから、比較の対象の特徴データに対応する証明書に記録された生成日時の際の別特徴データを入手し、且つ、比較対象の特徴データとその証明書に記録された生成方法とに基づいて比較対象の特徴データの別特徴データを生成し、その生成した別特徴データと上記入手した別特徴データとを比較する。なお、別特徴データを生成する手段は、定期的に（例えば1秒毎）別特徴データを生成しても良い。

【0015】好適な実施形態では、特徴データ又は別特徴データは、ハッシュ値である。

【0016】好適な実施形態では、1又は複数の情報処理装置において、第2の送り手段が、入手した証明書の

うち、生成した投票書類データに対応する証明書をその投票書類データに添付して、それを調達機関に送るようにする。

【0017】好適な実施形態では、開票の後に、投票参加者から不正があった旨（例えば調達機関で自分の投票書類データが改竄された旨）が報知（提起）されたときは、1又は複数の情報処理装置において、第1又は第2の入手手段が、上記報知（提起）を行なった投票参加者が保持する投票書類データを入手（例えばコンピュータネットワークを介してその投票書類データを受信）するよう

にし、比較する手段が、報知の内容が真実か否かを検知するために、上記報知を行なった投票参加者の投票書類データと、入手した暗号化投票書類データ又は暗号化特徴データのうち報知した投票参加者のものに該当するデータとを比較する。

【0018】好適な実施形態では、1又は複数の情報処理装置において、第2の送り手段が、投票書類データ又はその特徴データを暗号化して調達機関に送るようにする。

【0019】好適な実施形態では、第三者機関において、公開するための手段が、コンピュータネットワーク上に暗号化投票書類データ又は暗号化特徴データの各々を公開する。また、調達機関において、公開するための手段が、コンピュータネットワーク上に開票結果データを公開する。

【0020】好適な実施形態では、暗号化投票書類データ又は暗号化特徴データは、第三者機関の公開鍵で暗号化されており、第三者機関が、開票のときに第三者機関の秘密鍵を（調達機関、或いは1又は複数の情報処理装置に）発行する。

【0021】好適な実施形態では、1又は複数の情報処理装置において、第1の送り手段が、投票書類データ又はその特徴データを自分の（投票書類データを送るための情報処理装置の）秘密鍵又は共通鍵で暗号化して第三者機関に送り、第2の送り手段が、その自分の秘密鍵又は共通鍵で暗号化された投票書類データ又はその特徴データを第三者機関の公開鍵で更に暗号化して調達機関に送る。この場合、調達機関において、開票のとき

（より好適には開票日時）に第三者機関の秘密鍵を受けて、その秘密鍵で、第三者機関の公開鍵で更に暗号化された暗号化投票書類データ又は暗号化特徴データの各々を復号化する手段と、その復号化した暗号化投票書類データ又は暗号化特徴データの各々を、それらに対応する1又は複数の情報処理装置の公開鍵又は共通鍵で復号化する手段とが更に備えられる。

【0022】好適な実施形態では、1又は複数の情報処理装置と、第三者機関と、調達機関とがコンピュータネットワークを介して通信可能に接続されており、1又は複数の情報処理装置において、第1の送り手段が、投票書類データ又はその特徴データを暗号化してそれをコ

ンピュータネットワークを介して第三者機関に送信し、第2の送り手段が、投票書類データ、その特徴データ、暗号化投票書類データ、又は暗号化特徴データを暗号化してそれをコンピュータネットワークを介して調達機関に送信する。

【0023】好適な実施形態では、開票結果データには、開票の際に選出された投票書類データが含まれており、1又は複数の情報処理装置において、比較する手段が、選出された投票書類データと、入手した暗号化投票書類データ又は暗号化特徴データのうち上記選出された投票書類データに対応するデータとを比較する。

【0024】好適な実施形態では、投票書類データは、入札のときの提出書類の内容を示すデータである。

【0025】本発明に従う電子投票方法では、投票書類の内容を記録した投票書類データが暗号化されたものの各々を公開するためのステップと、投票書類データが調達される機関において調達された投票書類データの各々に基づく開票の結果を示すデータを公開するためのステップと、不正の有無を検知するために、公開された暗号化投票書類データと公開された開票結果データとを比較するステップとを有する。

【0026】好適な実施方法では、暗号化投票書類データの各々に対し、日時を付けてその投票書類データの存在を証明する証明書を生成するステップを更に有し、公開するためのステップが、生成した証明書の各々を、それらに対応する暗号化投票書類データに添付して公開するようし、比較するステップが、不正の有無を検知するために、公開された暗号化投票書類データに添付された証明書に付けられた日時と、開票の日時とを比較する。

【0027】

【発明の実施の形態】図3は、本発明の一実施形態に係る電子入札方式における全体的なシステム構成を示す。

【0028】各入札参加者が利用する端末装置11a、11b、11c、…、TTP（Trusted Third Party、第三者認証機関）15、及び調達機関13が、通信ネットワーク（典型的にはインターネット）27によって通信可能に接続されている。

【0029】端末装置11a、11b、11c、…は、典型的には、殆どどの会社にも設置されている汎用コンピュータ（例えばパーソナルコンピュータ）であって、後述する種々の動作、例えば、入札における提出書類の内容を示す文書データ（本明細書で言う「文書」は、文字データに限定されず、画像データ等も含む）のハッシュ値を生成したり（以下、ハッシュ文書という）、そのハッシュ文書をその入札参加者の秘密鍵で暗号化（以下、暗号化ハッシュ文書という）してそれをTTP15に送信したりする等の機能を備えている。以下の説明では、分かり易くするため、入札参加者を、「A社」、「B社」、「C社」の各会社とし、端末装置11a、1

11b、11cを、それぞれA社、B社、C社の「入札端末」と呼ぶことにする。

【0030】TTP15には、コンピュータネットワーク（例えばLAN）25が設けられており、そのネットワーク25には、入札支援サーバ19、タイムスタンプサーバ21、及びデータベース23が接続されている。

【0031】入札支援サーバ19は、主に、調達機関13での不正の可能性を無くすことに貢献している。即ち、入札支援サーバ19は、公開鍵・秘密鍵を作成して、はじめに、各入札参加社の上記暗号化ハッシュ文書を暗号化させるための公開鍵を調達機関13に送信し、開札時刻になったときに、公開鍵で暗号化された暗号化ハッシュ文書を復号化するための秘密鍵を調達機関13に送信する。また、入札支援サーバ19は、各入札端末11a、11b、11cからの暗号化ハッシュ文書を、後述するSHV証明書を添付して、インターネット27上に公開する。

【0032】タイムスタンプサーバ21は、主に、各入札端末提出11a、11b、11cからの入札文書の存在とその時刻、及び入札文書の内容が改竄されていないことを証明することを行なう。ここで、タイムスタンプサーバ21には、米国のSurety社が開発したDigital Notary Service（電子文書証明サービス、以下、DNS）における特表平10-508121号公報記載の技術が導入されている。即ち、タイムスタンプサーバ21は、各入札端末11a、11b、11cからの暗号化ハッシュ文書を受信したら、そのSHV（Super Hash Value、スーパーハッシュ値）を生成し、更に、その暗号化ハッシュ文書に対するSHV証明書を作成する。尚、SHVとは、DNSでのタイムスタンプ技術において生成されるハッシュ値のことである。

【0033】図4に、SHV証明書の構成の一例を示す。

【0034】タイムスタンプサーバ21は、例えば、暗号化ハッシュ文書のSHVを算出するためのSHV算出情報31、そのSHVを算出した日付・時刻（つまりそのSHVの存在を証明する日付・時刻）33、及びユーザID35などをSHV証明書37に掲載する。SHV算出情報31として、SHV算出の因子となる複数のハッシュ値や、その各ハッシュ値を用いるSHV算出の計算経路（計算手順）が示される。このSHV証明書に掲載されるSHV算出情報31、及び日付・時刻33は、例えば、暗号化ハッシュ文書が受信されて最初にSHVが算出されてから1秒後の、SHV算出情報、及び日付・時刻である。

【0035】SHV証明書37に基づいたSHVの算出方法に関しては、上記特表平10-508121号公報に記載のものを利用する。図5に、概略的にその一例を示す。

【0036】図4に示したSHV証明書37が添付され

ている暗号化ハッシュ文書200のSHVを、その証明書37に基づいて算出するときは、例えば次のようにして行なう。

【0037】まず、証明書37のSHV算出情報31に指定された第1の因子ハッシュ値（例えば「abcdef…」）203を抽出し、そのハッシュ値203と、暗号化ハッシュ文書のハッシュ値（例えば「ABCDE…」）201とを連結してハッシュをとり、連結したもののハッシュ値（例えば「AbCdeF…」）205を生成する。

【0038】次に、SHV算出情報31に指定された第2の因子ハッシュ値（例えば「aZbYcX…」）207と、上記生成したハッシュ値205とを連結してハッシュをとり、連結したもののハッシュ値（例えば「abBdcf…」）209を生成する。このようなハッシュ値の連結及び生成は、SHV算出情報31に指定された計算経路に従って行なっていく。

【0039】そして、最後は、最終的に生成したハッシュ値（例えばハッシュ値209）と、証明書37に記載されている日付・時刻（以下、当該時刻という）の1秒前のSHV211とを連結してハッシュをとり、当該時刻におけるSHV213を生成する。なお、当該時刻の1秒前のSHV211とは、後の説明でわかるとおり、タイムスタンプサーバ21が暗号化ハッシュ文書を受けてから入札審査が終了するまでの間に毎秒（つまり1秒毎に）作成するSHVにおいて、当該時刻の1秒前に該当するものである。

【0040】再び図3を参照して、タイムスタンプサーバ21は、入札端末11a、11b、11cからの各暗号化ハッシュ文書に対して、図4に示したようなSHV証明書を作成したら、それを入札支援サーバ19に渡す。これにより、この後、入札支援サーバ19は、上述したように、タイムスタンプサーバ21から渡された各SHV証明書を、入札端末11a、11b、11cからの暗号化ハッシュ文書にそれぞれ添付し、暗号化ハッシュ文書とSHV証明書のペアをインターネット27上に公開する。

【0041】また、タイムスタンプサーバ21は、各暗号化ハッシュ文書に対し、暗号化ハッシュ文書を受けてから入札審査が終了するまでの間、暗号化ハッシュ文書のSHVの生成を毎秒（つまり1秒毎に）行い、それをデータベース23に保存する。そして、タイムスタンプサーバ21は、不正に改竄されたか否かの検証が必要とされる暗号化ハッシュ文書の1秒毎のSHVを、インターネット27上に公開する。

【0042】TTP15は、入札支援サーバ19とタイムスタンプサーバ21の上述した各々の機能によって、この電子入札において不正が行われてもそれを確実に検証できるようにする。例えば、調達機関13が提出期限を過ぎているにも拘わらず不正に入札文書を受けたとしても、各入札参加社が、インターネット27上に公開さ

れている各入札文書（暗号化ハッシュ文書）のSHV証明書上の、文書存在を証明する日付・時刻を確認することで、その不正を検証できる。

【0043】調達機関13は、調達サーバ17を備えている。調達サーバ17は、TTP15からの公開鍵を受けてそれを各入札端末11a、11b、11cに配布し、その公開鍵によって暗号化された暗号化ハッシュ文書を各入札端末11a、11b、11cから受ける。調達サーバ17は、開札時刻になったら、TTP15から秘密鍵を受け、その秘密鍵で、それら暗号化された暗号化ハッシュ文書を復号化する。そして、調達サーバ17は、入札参加社の秘密鍵で暗号化された各暗号化ハッシュ文書を、その入札参加社の公開鍵で復号化して、各入札に対する審査を行なえるようにする。また、その審査が終了して落札社が決定したときは、調達サーバ17は、入札の審査結果（例えば、決定された落札社の会社名、落札社の入札文書等）を、インターネット27上に公開する。

【0044】以下、図6～図10を参照して、上述したシステム構成において行なわれる電子入札の手順を具体的に説明する。

【0045】まず、図6に示すように、TTP15の入札支援サーバ19が、公開鍵・秘密鍵を作成し（ステップS21）、そのうち公開鍵のみを調達機関13に送付する（S22）。調達機関13の調達サーバ17は、TTP15からの公開鍵を、各入札端末11a、11b、11cに配布する（S24、25、26）。

【0046】その後、各入札端末11a、11b、11cは、図7に示すように、入札する文書のハッシュをとってそのハッシュ値を生成し（ステップS27、28、29）、それを自社の秘密鍵で暗号化する（S30、31、32）。そして、各入札端末11a、11b、11cは、自社の秘密鍵により暗号化した暗号化ハッシュ文書を、インターネット27を介してTTP15に送信する（S33、S34、S35）。

【0047】TTP15では、図8に示すように、タイムスタンプサーバ21が、各入札端末11a、11b、11cからの暗号化ハッシュ文書について、それぞれに図4に示したようなSHV証明書を作成し（ステップS36）、それを入札支援サーバ19に渡す（S37）。入札支援サーバ19は、各暗号化ハッシュ文書に、タイムスタンプサーバ21から渡されたSHV証明書をそれぞれ添付し、暗号化ハッシュ文書とSHV証明書のペアをインターネット27上に公開する（S38）。この公開の方法としては、例えばこの図に示すように、入札支援サーバ19は、TTP15のホームページ101上に、各参加社の暗号化ハッシュ文書とSHV証明書とのペア103a、103b、103cを掲載する。各参加社は入札端末11a、11b、11cを利用して、TTP15によって公開された全ての参加社のデータ103

a、103b、103cをダウンロードする（S39、40、41）。

【0048】一方で、TTP15のタイムスタンプサーバ21は、各入札端末11a、11b、11cからの暗号化ハッシュ文書について、例えば上記特表平10-508121号公報に記載の方法を利用して、毎秒（つまり1秒毎に）SHVを算出する（S42）。タイムスタンプサーバ21は、その方法により算出した各暗号化ハッシュ文書の毎秒のSHVを、データベース23に保存すると共に（S43）、インターネット27上に公開する（S44）。この公開の方法としては、例えばこの図に示すように、TTP15のホームページ110を用意し、そのホームページ110上に、所望のSHV証明書のユーザIDを入力させて所望の参加社の公開SHVデータ111を表示する。公開SHVデータ111は、TTP15が入札文書を受けてから入札審査が終了するまでの毎秒の暗号化ハッシュ文書のSHVである。尚、この公開SHVデータ111は、CD-ROM等の記録媒体に記録させて、その記録媒体を全参加社に配布する等するようにしても良い。

【0049】各入札端末11a、11b、11cは、調達機関13に入札するときは、図9に示すように、暗号化ハッシュ文書に電子署名し（ステップS45、46、47）、それを調達機関13から配布されたTTP15発行の公開鍵を使用して暗号化する（S48、49、50）。そして、各入札端末11a、11b、11cは、その暗号化ハッシュ文書を調達機関13に送信することで入札を行なう（S51、52、53）。なお、この図において、各入札端末11a、11b、11cは、自分の暗号化ハッシュ文書に対応するSHV証明書をTTP15から入手し、そのSHV証明書と共に、自分の暗号化ハッシュ文書を調達機関13に送信することもできる。これにより、調達機関13は、各入札端末11a、11b、11cからSHV証明書付きの暗号化ハッシュ文書を受けることになるので、それらSHV証明書に基づいて上記方法で各暗号化ハッシュ文書のSHVを求め、求められたSHVと、公開SHVデータ111からSHV証明書に記録された日付・時刻のSHVを取得したものとを比較することで、各入札端末11a、11b、11cから送られて来た入札文書が不当に改竄されていないかどうかを確認することができる。また、調達機関13は、後述する入札審査結果の公開のときに、SHV証明書も併せて公開することができるので、各参加社に対する透明性をより高めることができる。

【0050】開札時刻になったら、図10に示すように、TTP15の入札支援サーバ19が、秘密鍵を調達機関13に送付する（ステップS54）。調達機関13の調達サーバ17は、TTP15からの秘密鍵を使用して、TTP15の公開鍵によって暗号化されている各入札端末11a、11b、11cからの暗号化ハッシュ文

書を復号化する(S55)。それにより、復号化された各暗号化ハッシュ文書は、各参加者の秘密鍵によって暗号化されているハッシュ文書となる。そこで、調達サーバ17は、それらの暗号化ハッシュ文書を、その入札参加社の公開鍵で復号化して(S56)、各入札に対する審査を可能な状態にする。調達サーバ17は、その審査が終了して落札する社が決定したときは、その審査の結果を各入札参加社に対して公開する(S57)。この公開の方法としては、例えばこの図に示すように、調達サーバ17は、調達機関13のホームページ105上に、入札審査の結果、例えば落札社の入札文書(納品物に関する提案書、技術仕様書、受注金額など)107を掲載する。勿論、調達サーバ17は、入札審査の結果として、全ての入札参加社の入札文書をホームページ105上に掲載するようにしてもよい。この場合は、後述する不正の検証において、各入札参加社は、入札端末11a、11b、11cを利用して、その入札審査結果をダウンロードし、その審査結果として(つまり開札後)の全ての入札参加社の入札文書と、既に保持している開札前の全参加社の入札文書(暗号化ハッシュ文書)とを比較して、不正の有無を検証することができる。

【0051】各入札参加社は、入札端末11a、11b、11cを利用して、この電子入札において、不正が行なわれたか否かを検証できるように、落札社の入札文書107をダウンロードする(S58、59、60)。

【0052】この実施形態における電子入札では、従来検証できなかった以下の不正を検証することができる。その不正の検証について説明する。

【0053】(1) 調達機関3が、受け付けた入札文書を開札後に改竄すること。

【0054】これについては、各入札参加社が、入札端末11a、11b、11cを利用して検証できる。それについて、図11を参照して説明する。

【0055】入札端末11a、11b、11cは、図10のステップS58、59、60で、落札社の入札文書107をダウンロードした。そこで、入札端末11a、11b、11cは、その落札社入札文書107のハッシュをとって、開札後の落札社入札文書のハッシュ値を生成する(ステップS61)。

【0056】また、入札端末11a、11b、11cは、図8のステップS39、40、41で、全参加社の暗号化ハッシュ文書及びそのSHV証明書のペア103a、103b、103cをダウンロードした。各暗号化ハッシュ文書は、その参加社の秘密鍵で暗号化された文書である。そこで、入札端末11a、11b、11cは、ダウンロードした暗号化ハッシュ文書のうち落札社の暗号化ハッシュ文書を、その落札者の公開鍵で復号化して、開札前の落札社入札文書のハッシュ値を得る。

【0057】入札端末11a、11b、11cは、落札社入札文書の、開札後のハッシュ値と開札前のハッシュ

値とを比較し、それらが一致していなければ、落札社の入札文書は開札後に改竄されたと判断する(S63)。

【0058】このようにして、各入札参加社は、この電子入札における不正を検証することができる。

【0059】(2) 調達機関3が、提出期限が過ぎているにも拘わらず入札文書を受け付けること。

【0060】これについては、各入札参加社が、入札端末11a、11b、11cを利用して検証できる。入札端末11a、11b、11cは、落札社のSHV証明書に記録されている日付・時刻の正当性を証明し、その時刻が開札時刻の前・後のどちらであるかを参加社に確認してもらうことでこの不正を検証できるようにする。これについて、図12を参照して説明する。

【0061】入札端末11a、11b、11cは、図11に示したステップS63の動作を終えた後に、この不正の検証を行なうことができる。入札端末11a、11b、11cは、図11のステップS63の後、公開SHVデータ111が掲載されているホームページ110

(図8参照)にアクセスし、落札社のSHV証明書に記録されているユーザIDをキーに、落札社の公開SHVデータ111を取得し、そのデータから落札社のSHV証明書の日付・時刻の正当性を証明するために必要なSHVを得る(ステップS64)。その必要なSHVは、当該時刻(つまり証明書の日付・時刻)でのSHVとその時刻の1秒前のSHVである。入札端末11a、11b、11cは、落札社の暗号化ハッシュ文書、それに添付されているSHV証明書中のSHV算出情報(図4参照)、及び当該時刻の1秒前のSHVを用いて、例えば図5を参照して説明した方法により、当該時刻のSHVを算出する(S65)。

【0062】その後、入札端末11a、11b、11cは、その算出した当該時刻のSHVと、ステップS64で公開データ111から取得した当該時刻のSHVとを比較し、それらが一致していれば、落札社のSHV証明書中の日付・時刻は正当なものであると証明する(S66-a)。そして、その証明された時刻と開札時刻とを比較し、その証明された時刻が開札時刻の後であれば、落札社の入札文書は提出期限が過ぎているにも拘わらず調達機関13で不正に受けられたものと判断する(S66-b)。

【0063】(3) ある参加社が、入札又は開札後に、自分の手元にある入札文書の内容を不正に改竄すること。

【0064】例えば、B社が、落札社決定後に自分の手元にある入札文書を不正に改竄しその入札文書が本物であると主張しているとする。他の参加社であるA社、C社は、自社の入札端末11a、11cを利用してその主張は正当なものか否かを検証できる。それについて、図13を参照して説明する。

【0065】まず、B社が、自社の入札端末11bを利

10

20

30

40

50

用して、本物であると主張しているB社主張入札文書300をインターネット27上に公開するようにする(ステップS67)。

【0066】他の参加社であるA社、C社は、自社の入札端末11a、11cを利用して、B社主張入札文書300をダウンロードし(S68、S72)、B社主張入札文書300のハッシュ値を生成する(S69、S73)。その後、以前にダウンロードしたB社の暗号化ハッシュ文書をB社の公開鍵で復号化して、B社の当初の入札文書のハッシュ値を得る(S70、S74)。そして、そのB社の当初入札文書のハッシュ値と、ステップS69、73で生成したB社主張入札文書のハッシュ値とを比較し、それらが一致していなければ、B社の主張は不当であると判断する(S71、S75)。

【0067】このように、ある参加社が入札又は開札後に自分の手元にある入札文書の内容を不正に改竄しても、他の参加社がその不正を検証することができる。これにおいて、B社が上記主張を正当であるとするためには、他の参加社A社、C社が各々保有するB社の暗号化ハッシュ文書の全てをB社主張の入札文書に取り替えなければならない。これを行なうのは実質的に不可能なので、上記不当な主張が行なわれることを未然に防ぐことが図れる。

【0068】上述した実施形態によれば、従来検証することができなかった上記種々の不正を、各参加社が検証できるので、電子入札の信頼性を高めるられると共に、上記種々の不正が行なわれることを未然に防ぐことが図れる。

【0069】また、上述した実施形態によれば、TTP15が、不正の検証に必要なデータ(各参加者の開札前の入札文書データ(暗号化ハッシュ文書)、SHV証明書、公開SHVデータ111)を公開する。このため、極めて信頼性の高いデータが公開されるので入札における透明性が高まり、また、裁判ではそのデータを証拠としても利用できる可能性が高いので、安全性・信頼性の高い電子入札が可能になる。

【0070】以上、本発明の好適な幾つかの実施形態を説明したが、これらは本発明の説明のための例示であって、本発明の範囲をこれらの実施例にのみ限定する趣旨ではない。本発明は、他の種々の形態でも実施することが可能である。すなわち、本発明を入札に適用としたときの一実施形態の説明からもわかるように、本発明は、電子投票において行なわれ得る実質的に全ての不正を検証できるものである。従って、本発明は、あらゆる投票の態様に適用することが可能であり、選挙のような不正

が絶対にあってはならないものにこそ本発明は適用価値がある。仮に、選挙に適用すれば、信頼性・安全性の高い選挙が保証されるだけでなく、選挙権者は通信端末装置さえ持っていればどこからでも投票可能になるので、わざわざ選挙会場まで足を運ぶ必要が無くなり、投票率の向上が期待できる。

【図面の簡単な説明】

【図1】従来の電子入札における動作説明図。

【図2】従来の電子入札における動作説明図。

【図3】本発明の一実施形態に係る電子入札方式における全体的なシステム構成を示すブロック図。

【図4】SHV証明書の構成の一例を示す図。

【図5】SHV証明書に基づいたSHVの算出方法を説明するための図。

【図6】各入札端末11a、11b、11cにTTP15の公開鍵が配布されるとき動作を示す図。

【図7】各入札端末11a、11b、11cがTTP15に暗号化ハッシュ文書を送信するとき動作を示す図。

【図8】TTP15が各参加社の暗号化ハッシュ文書やそのSHVを公開するとき動作を示す図。

【図9】各入札端末11a、11b、11cによって入札が行なわれるとき動作を示す図。

【図10】入札審査の結果が公開されるとき動作を示す図。

【図11】各入札端末11a、11b、11cが、調達機関3が受け付けた入札文書を開札後に改竄することを検証するとき動作を示すフローチャート。

【図12】各入札端末11a、11b、11cが、調達機関3が提出期限を過ぎているにも拘わらず入札文書を受け付けることを検証するとき動作を示すフローチャート。

【図13】ある参加社が入札又は開札後に自分の手元にある入札文書の内容を不正に改竄することを検証するとき動作を示すフローチャート。

【符号の説明】

11a、11b、11c 入札端末

13 調達機関

15 TTP

17 調達サーバ

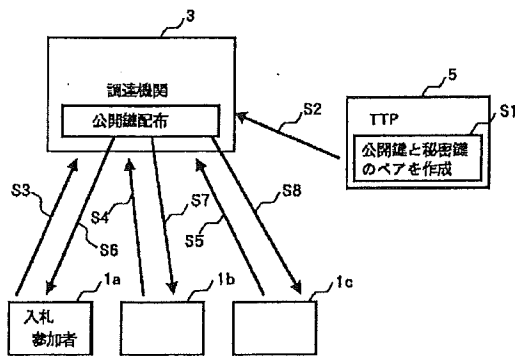
19 入札支援サーバ

21 タイムスタンプサーバ

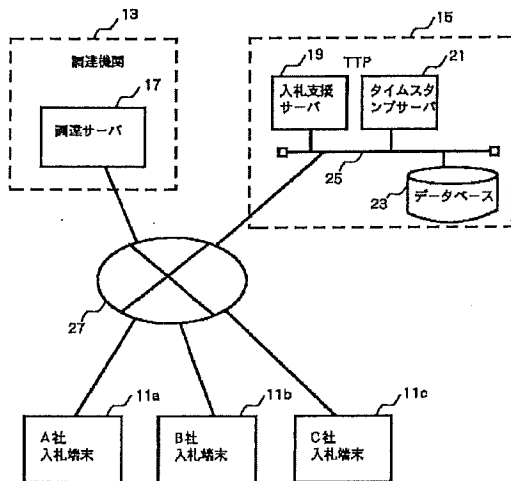
27 インターネット

37 SHV証明書

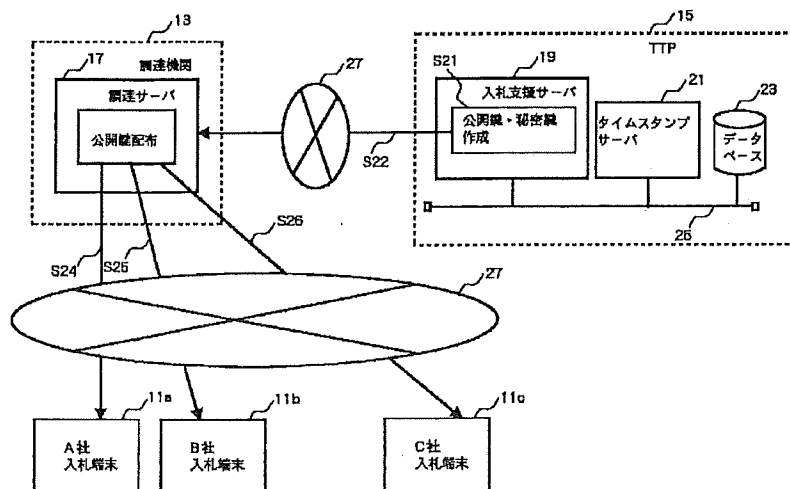
【図1】



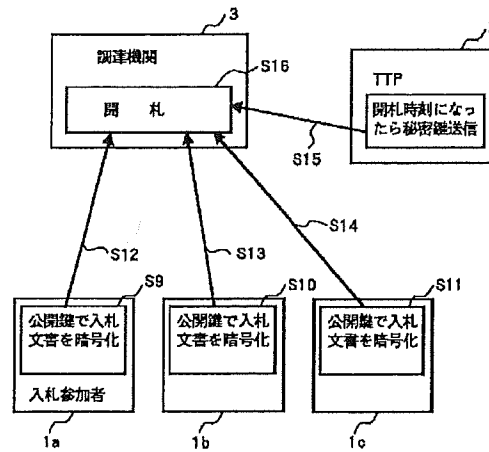
【図3】



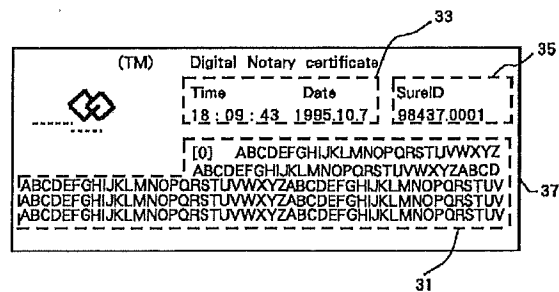
【図6】



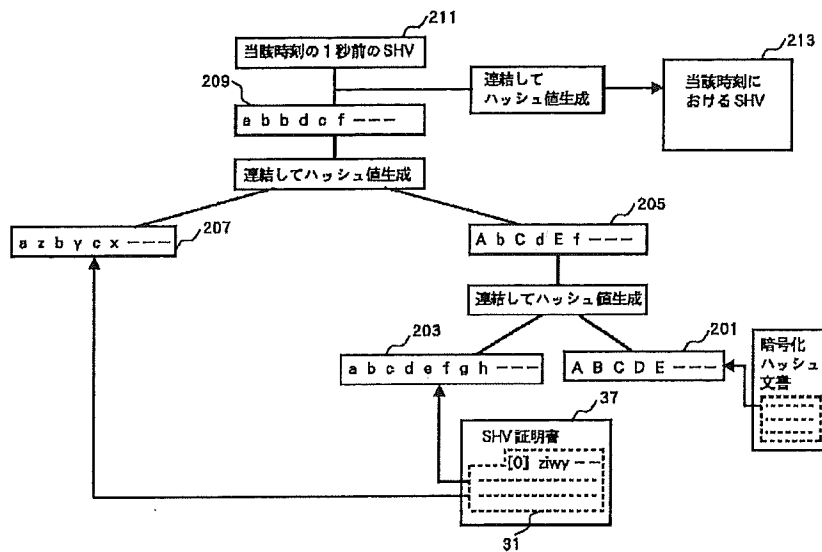
【図2】



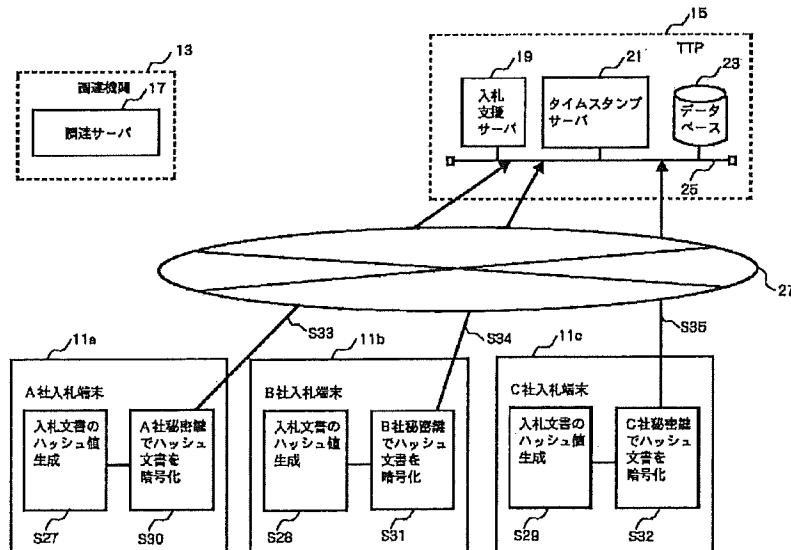
【図4】



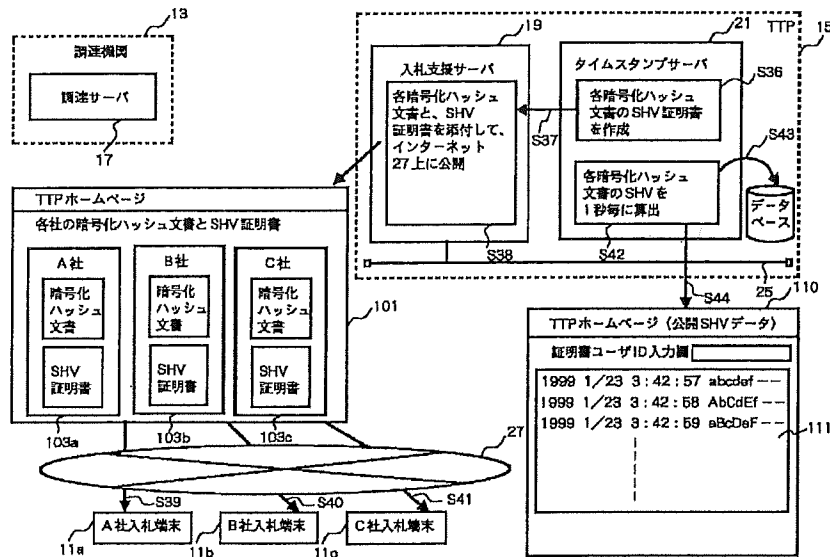
【図5】



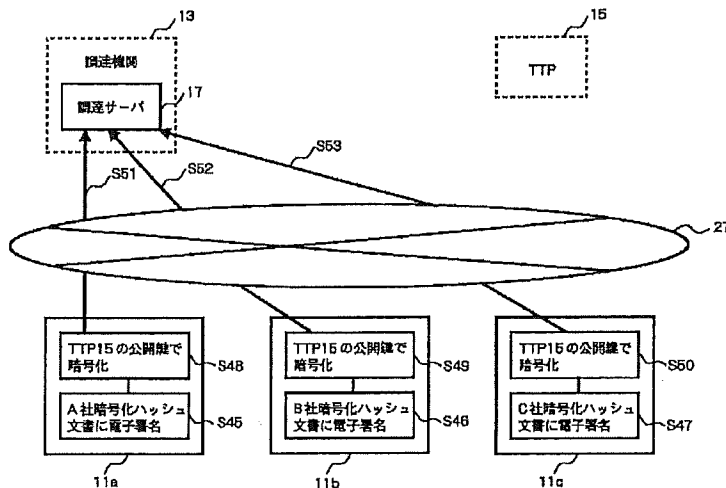
【図7】



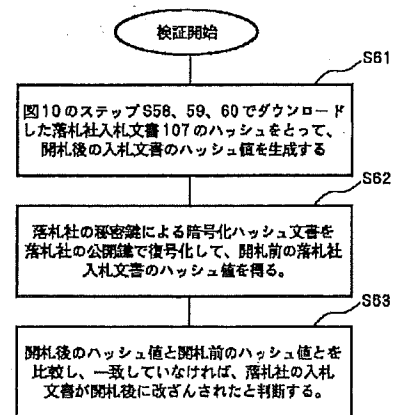
【図8】



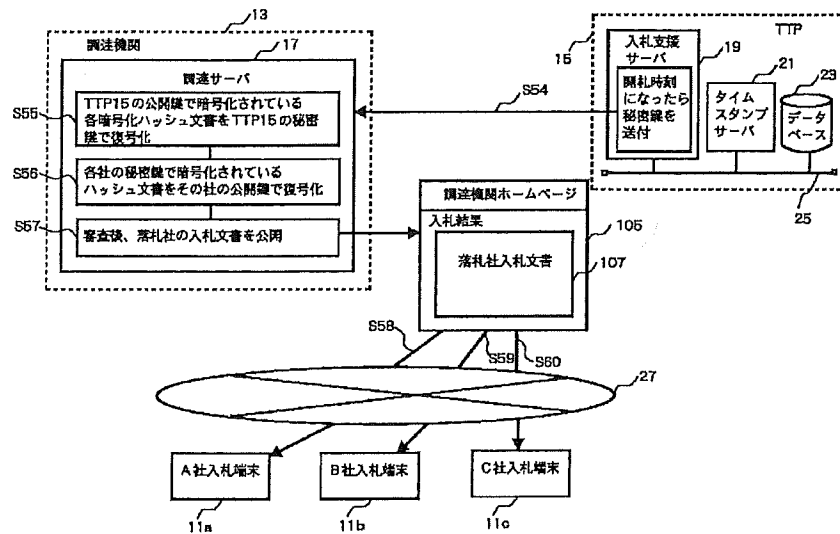
【図9】



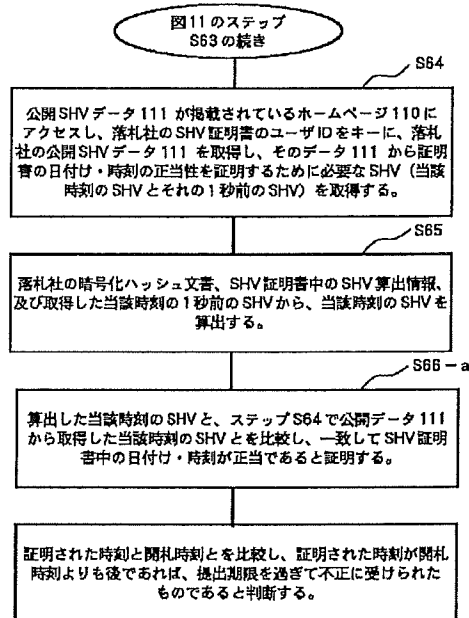
【図11】



【図10】



【図12】



【図13】

